(12) INTERNATIONAL [redacted]ICATION PUBLISHED UNDER THE PATENT [redacted]PERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 January 2002 (03.01.2002)

PCT

(10) International Publication Number
WO 02/01516 A2

(51) International Patent Classification[7]: G07F 7/00

(21) International Application Number: PCT/US01/17704

(22) International Filing Date: 1 June 2001 (01.06.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/603,169 26 June 2000 (26.06.2000) US

(71) Applicant *(for all designated States except US)*: **INTEL CORPORATION** [US/US]; 2200 Mission College Boulevard, Santa Clara, CA 95052 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **AUCSHITH, David** [US/US]; 6995 SW Labor Road, Portland, OR 97225 (US). **SULLIVAN, Robert, Jr.** [US/US]; 6930 Corte Mercado, Pleasanton, CA 94566 (US).

(74) Agents: **SZE, James, Y., C.** et al.; Pillsbury Winthrop, 1100 New York Avenue, NW, 9th Floor East Tower, Washington, DC 20005 (US).

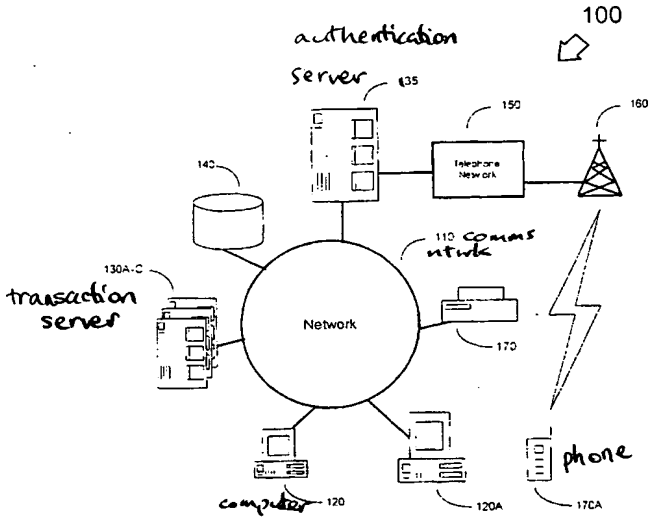
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR USING A CELLULAR TELEPHONE AS AN AUTHENTIFICATION DEVICE



(57) Abstract: A method and apparatus for authenticating a participant of an electronic transaction. The participant is pre-registered with a caller database, and the participant's wireless telephone number is unique to a particular user. When an authentication server is notified of a transaction, it generates a transaction pin for the transaction participant and forwards the transaction pin to the participant via a network. The participant calls the authentication server via a wireless phone. The authentication server identifies the wireless telephone number and prompts the caller for the transaction pin. When combined with a known transaction pin and a unique wireless telephone number, a wireless phone user can be authenticated as a valid participant of an on-line transaction.

WO 02/01516 A2

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

METHOD AND APPARATUS FOR USING A CELLULAR TELEPHONE AS AN AUTHENTIFICATION DEVICE

BACKGROUND

Field of the Invention

Aspects of the present invention relate in general to authenticating a user, and in particular to a method and system of verifying users in electronic transactions.

Description of the Related Art

The problem of authenticating the identity of people has existed for hundreds of years. In conventional transactions, authentication can be accomplished in a number of ways. For example, a commonly accepted form of identification document, such as a picture identifier (a "picture ID"), could be used to verify a person's identity.

However, with the advent of the Internet, an ever-increasing number of electronic (or "e-commerce") transactions take place. With electronic transactions, parties to a transaction cannot see the other parties, and often never meet or know the other parties at all.

Moreover, conventional methods of verifying identity in an electronic-transaction often involve conveying personal information that only a valid person should know. Examples include using credit card numbers, social security numbers, address and other personal information. As personal information proliferates, privacy experts and the public are justifiably worried about the spread of such data. Even worse, as personal information proliferates, the information becomes "tainted" and too commonly known to serve as valid authenticators of personal identity.

Consequently, the problem of authenticating the identity of a transaction participant is non-trivial and difficult.

Therefore, what is needed is a method of securely authenticating users in an electronic transaction.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 illustrates an embodiment of a system that authenticates users in an electronic transaction.

FIG. 2 is a block diagram of an apparatus that authenticates users in an electronic transaction.

FIG. 3 is a block diagram of an embodiment that authenticates users in an electronic transaction.

FIG. 4 is flowchart of a method that requests authentication of users in an electronic transaction.

FIGS. 5a and 5b are flowcharts of a method that authenticates users in an electronic transaction.

DETAILED DESCRIPTION

FIG. 1 is a simplified functional block diagram depicting system 100, constructed and operative in accordance with an embodiment of the present invention. System 100 is configured to authenticate a user in an electronic transaction. Electronic transactions are any transactions that take place over a computer network (i.e., an "on-line" transaction). Examples of such transactions include, but are not limited to, any sale or purchase of goods and services, or any operation that involves the electronic authorization of a party. An example of the former is purchasing a book, compact disk, or any other goods or

services, via an Internet browser on the World-Wide-Web ("WWW" or the "web"). An example of the latter transaction is the doctor's approval of a medical prescription being filled by an electronic pharmacy.

The method relies on the fact that a user is pre-registered with a caller database, and the user's wireless telephone number is unique to a particular user. When combined with a known transaction code (e.g., Personal Identification number, PIN), which is sent to a user as part of the on-line/network transaction, a wireless phone user can be authenticated as a participant of the on-line transaction.

In system 100, computer 120 and an authentication server 135 are connected to a communications network 110. The network 110 may also include other networkable devices known in the art, such as other computers 120, servers 130, printers 125 and storage media 140. It is well understood in the art, that any number or variety of computer networkable devices or components may be coupled to the network 110 without inventive faculty. Examples of other devices include, but are not limited to, servers, computers, workstations, terminals, input devices, output devices, printers, plotters, routers, bridges, cameras, sensors, or any other such device known in the art. Computer 120 may be of any kind known in the art that are able to communicate on the network 110. Servers 130A-C may be any servers known in the art, including web, database, print, or application servers. More importantly, servers 130A-C may generate, originate, or participate in an electronic transaction that requires user authentication. A server participating in an electronic transaction is referred to as a "transaction server" 130.

Network 110 may be any communication network known in the art, including the Internet, a local-area-network (LAN), a wide-area-network (WAN), or any system that links a computer to an authentication server 135. Further, network 110 may be of

configured in accordance with any topology known in the art, including star, ring, bus, or any combination thereof.

Authentication server 135 is connected to a telephone network 150 that supports Calling Number Delivery (CND), also known as Caller ID (CID). Telephone network 150 may be configured as a packet switch telephone network (PSTN), plain ordinary telephone service (POTS), Integrated Services Digital Network (ISDN), or any other telephone network 150 known in the art that supports caller ID. In turn, telephone network 150 is connected to a wireless telephone system 160 that also supports Caller ID.

Each user in system 100 has a wireless phone 170. Authentication server 135 knows each user's wireless telephone number and stores the wireless telephone number in a caller database. In some embodiments, transaction server 130, requiring user authentication, may also be the same apparatus as the authentication server 135, without any loss of functionality.

Embodiments will now be disclosed with reference to a functional block diagram of an exemplary authentication server 135 of FIG. 2. Authentication server 135 runs a multi-tasking operating system and includes at least one central processing unit (CPU) 102. CPU 102 may be any microprocessor or micro-controller as is known in the art. For example, CPU 102 may be a microprocessor, such as the Pentium III™ processor manufactured by Intel Corporation. The software for programming the CPU may be found at a computer-readable storage medium 140 or, alternatively, from another location across network 110. CPU 102 is connected to computer memory 118. Authentication server 135 is controlled by an operating system (OS) that is executed within computer memory 118.

CPU 102 communicates with a plurality of peripheral equipment, including computer network interface 116 and telephone network interface 112. Additional

peripheral equipment may include a display 104, manual input device 106, storage medium 140, microphone 108, and data input port 114. Display 104 may be a visual display such as a cathode ray tube (CRT) monitor, a liquid crystal display (LCD) screen, touch-sensitive screen, or other monitors as are known in the art for visually displaying images and text to a user. Manual input device 106 may be a conventional keyboard, keypad, mouse, trackball, or other input device as is known in the art for the manual input of data. Storage medium 140 may be a conventional read/write memory such as a magnetic disk drive, floppy disk drive, compact-disk read-only-memory (CD-ROM) drive, transistor-based memory or other computer-readable memory device as is known in the art for storing and retrieving data. Significantly, storage medium 140 may be remotely located from CPU 102, and be connected to CPU 102 via a network 110 such as a local area network (LAN), a wide area network (WAN), or the Internet.

Microphone 108 may be any suitable microphone as is known in the art for providing audio signals to CPU 102. In addition, a speaker (not shown) may be attached for reproducing audio signals from CPU 102. It is understood that microphone 108 and speaker may include appropriate digital-to-analog and analog-to-digital conversion circuitry as appropriate.

Data input port 114 may be any data port as is known in the art for interfacing with an external accessory using a data protocol such as RS-232, Universal Serial Bus (USB), or Institute of Electrical and Electronics Engineers (IEEE) Standard No. 1394 ('Firewire').

Network interface 116 may be any interface as known in the art for communicating or transferring files across a computer network, examples of such networks include Transmission Control Protocol/Internet Protocol (TCP/IP), Ethernet, Fiber Distributed Data Interface (FDDI), token bus, or token ring networks. In addition, on some systems,

network interface 116 may consist of a modem connected to the data input port 114. Similarly, telephone network interface 112 provides connectivity to authentication server 135 to communicate with a telephone network 150. Thus, the telephone network interface 112 allows the authentication server 135 to communicate and process input from a telephone line.

FIG. 3 is an expanded functional block diagram of CPU 102 and storage medium 140. It is well understood by those in the art, that the functional elements of FIG. 3 may be implemented in hardware, firmware, or as software instructions and data encoded on a computer-readable storage medium 140. As shown in FIG. 3, central processing unit 102 is functionally comprised of a data processor 202, an application interface 204, a transaction processor 206, and a call handler 210. Data processor 202 interfaces with display 104, manual input device 106, storage medium 140, microphone 108, data input port 114, Internet network interface 116, and telephone network interface 112. The data processor 202 enables CPU 102 to locate data on, read data from, and write data to, these components.

Application interface 204 enables CPU 102 to take some action with respect to a separate software application or entity. For example, application interface 204 may take the form of a windowing user interface, as is commonly known in the art.

Transaction processor 206 handles an electronic commerce transaction. Transaction processor 206 approves or disapproves of transactions depending upon the verification of a user by call handler 210. The results of transaction processor 206 may be recorded on storage media 140 as a transaction log 242. Call handler 210 may be further comprised of a caller ID processor 212 and a caller verifier 214. These components of call

handler 210 interact with a known caller database 244, and may best be understood with respect to the flowcharts of FIGS. 4, 5a and 5b, as described below.

FIG. 4 is a flow diagram depicting process 300, constructive and operative in accordance with an embodiment of the present invention. As shown in block 302, process 300 initially determines whether transaction server 130 is participating in an electronic transaction that requires a user authentication. This determination may be accomplished by any means known in the art, including a table-look-up of a list of electronic transactions that require user authentication, or may be embedded within a program being executed by transaction server 130. Process 300, in block 304, may suspend the transaction while the user is being authenticated.

In block 306, process 300 initiates transaction server 130 to sends authentication request (also known as a "transaction notification") to authentication server 135. The authentication request may comprise a user identifier and a transaction identifier. The user identifier can be any information that identifies the user as a party of the transaction, including: name, social security number, or any other similar identifier. The transaction identifier identifies the transaction that requires the authentication. Additionally, in some embodiments, the user's electronic mail address may also be encoded within the authentication request. The notification is conveyed to authentication server 135 via network 110. In embodiments that combine authentication server 135 with transaction server 130, the notification may be sent internally within the device itself.

In block 310, process 300 waits for authentication server 135 to respond to the authentication request. Upon receiving a response from authentication server 135, process 300 determines whether the received response indicates that the user is authenticated.

When the user is authenticated by the authentication server 135, the transaction is approved, block 312. Otherwise, the transaction is disallowed in block 314.

FIG. 5a and FIG. 5b are flow diagrams depicting process 400 and 450, respectively. Process 400 and 450 describe the authentication sequence from the point of view of authentication server 135. Authentication server 135 receives an authentication request or transaction notification from the transaction server 130 in block 401. Transaction processor 206 decodes the user identifier and the transaction identifier from the authentication request. In block 403, transaction processor 206 generates a transaction PIN that comprises a sequence of numbers, between zero and nine. The sequence is used in conjunction with a user's wireless telephone number to authenticate the user's participation in a transaction. Note that in some embodiments, the transaction PIN may contain alphanumeric characters including as well the symbols "*" and "#", words or a sequence of letters that can be entered via a telephone keypad.

Embodiments that generate numeric transaction PINs may generate a pseudo-random number by any means known in the art. Embodiments that use letters may generate a pseudo-random series of letters and numbers or may use a dictionary to generate the transaction pin. Some embodiments look up the user's entry in the caller database 244, and append or store the transaction identifier and the transaction pin as fields in the caller database 244, or as part of the transaction log 242.

In block 405, process 400 transmits the transaction PIN to the user. The transaction PIN is sent to the user by transaction processor 206 via network interface 116 and network 110. In all embodiments, the user is provided a telephone number that they are required to call to authenticate themselves as a valid user in the transaction. The telephone number provided is connected to authentication server 135 via telephone network 150. In some

embodiments, the telephone number is conveyed by looking up the electronic mail address of the user in a caller database 244, and then electronic-mailing the user convey the telephone number. Other embodiments include using the electronic mail address encoded within the authentication request. Still other embodiments display the transaction PIN before the user via a World-Wide-Web page.

Process 450 of FIG. 5b authenticates the user by matching the user's caller-identified wireless phone number with the transaction PIN provided by process 400 in FIG. 5a. The user calls the provided telephone number, reaching authentication server 135. Authentication server 135 receives the call from the user at block 402. In block 404, Authentication server 135 identifies the user by matching the user as a caller from a certain wireless phone number via caller ID. Authentication server 135 receives the call via its telephone network interface 112. The call is then routed to call handler 210. In some embodiments, the caller ID signal delivered as a V.23 modem signal between the 1st and 2nd ring cycles. In embodiments connected to an ISDN line, the Caller ID is delivered over the D (signaling) channel at the initial onset of call setup in compliance with ITU-T specification Q.81.3. Regardless of the implementation of caller ID, the caller ID processor 212 derives the user's telephone number. Caller verifier 214 takes the telephone number and looks up the caller identity in caller database 244.

If the telephone number cannot be determined, or the caller is not a known user of the system (as determined by caller database 244), the phone call is ignored, and authentication server 135 hangs up, block 408.

Otherwise, if the caller is identified as a known user in caller database 244, the caller is prompted to enter the transaction PIN, block 410.

If the transaction PIN entered by the caller matches the one sent to the user by process 400, as determined by transaction processor 206, the user is authenticated, and transaction server 130 is informed of the authentication by internet network interface 116, block 414.

If the transaction PIN entered by the caller does not matches the one sent to the user, as determined by transaction processor 206, the authentication fails, and transaction server 130 is informed of the failure by the internet network interface 116. In some embodiments users can be offered an opportunity to re-enter the transaction PIN, block 416.

The outcome of the authentication may be recorded in a transaction log 242.

The previous description of the embodiments is provided to enable any person skilled in the art to practice the method. The various modifications to these embodiments will be readily apparent to those skilled in the art, and the generic principles defined herein may be applied to other embodiments without the use of inventive faculty. Thus, the present invention is not intended to be limited to the embodiments shown herein, but is to be accorded the widest scope consistent with the principles and novel features disclosed herein.

WHAT IS CLAIMED IS:

1. An apparatus comprising:

a first network interface, connected to a computer network, configured to receive a transaction notification, the transaction notification containing a user identifier that identifies a participant to an electronic transaction;

a processor, connected to the first network interface, configured to match the user identifier to a user phone number in a caller database and generate a transaction PIN, the first network interface forwards the transaction pin the participant; and

a second network interface, connected to the processor and a telephone network, configured to receive a phone call from a caller with a caller phone number, wherein the processor prompts the caller for a caller pin, the processor identifies the caller telephone number, and the processor authenticates the participant when the caller phone number and user phone number match and the transaction pin and the caller pin match.

2. The apparatus of claim 1, the processor further comprising:

a transaction processor that matches a user phone number to the user identifier, generates a transaction pin, and authenticates the participant when the caller phone number and user phone number match and the transaction pin and the caller pin match.

3. The apparatus of claim 2, the processor further comprising:

a caller ID processor, connected to the transaction processor, configured to identify the caller telephone number.

4. The apparatus of claim 3, the processor further comprising:

a caller verifier, connected to the transaction processor, configured to match the user identifier to the user phone number in the caller database.

5. A method comprising:

receiving a transaction notification via a first network interface, the transaction notification containing a user identifier that identifies a participant to an electronic transaction;

matching a user phone number to the user identifier;

generating a transaction pin;

forwarding the transaction pin the participant;

receiving a phone call via from a caller with a caller phone number via a second network interface;

prompting the caller for a caller pin;

verifying that the caller is a user when the caller phone number and user phone number match; and

verifying that the caller is a participant to the electronic transaction when the transaction pin and the caller pin match.

6. The method of claim 5, further comprising:

authenticating the user of the electronic transaction when the caller is verified as a user and when the caller is verified as a participant to the electronic transaction.

7. The method of claim 6, further comprising:

informing a transaction server whether the user of the electronic transaction is authenticated.

8. The method of claim 7, further comprising:

canceling the electronic transaction when the user of the electronic transaction is not authenticated.

9. The method of claim 8, further comprising:

recording an outcome of the user authentication in a transaction log.

10. The method of claim 9, wherein generating a transaction pin is accomplished by generating a pseudo-random combination of numbers and letters.

11. The method of claim 9, wherein generating a transaction pin is accomplished by generating a pseudo-random selection of a word or words from a dictionary.

12. A computer-readable medium encoded with data and instructions, the data and instructions causing an apparatus executing the instructions to:

receive a transaction notification via a first network interface, the transaction notification containing a user identifier that identifies a participant to an electronic transaction;

match a user phone number to the user identifier;

generate a transaction pin;

forward the transaction pin the participant;

receive a phone call via from a caller with a caller phone number via a second network interface;

prompt the caller for a caller pin;

verify that the caller is a user when the caller phone number and user phone number match;

verifying that the caller is a participant to the electronic transaction when the transaction pin and the caller pin match.

13. The computer-readable medium of claim 12 further encoded with data and instructions, the data and instructions causing an apparatus executing the instructions to:

authenticate the user of the electronic transaction when the caller is verified as a user and when the caller is verified as a participant to the electronic transaction.

14. The computer-readable medium of claim 13 further encoded with data and instructions, the data and instructions causing an apparatus executing the instructions to:

inform a transaction server whether the user of the electronic transaction is authenticated.

15. The computer-readable medium of claim 14 further encoded with data and instructions, the data and instructions causing an apparatus executing the instructions to:

cancel the electronic transaction when the user of the electronic transaction is not authenticated.

16. The computer-readable medium of claim 15 further encoded with data and instructions, the data and instructions causing an apparatus executing the instructions to:

record an outcome of the user authentication in a transaction log.

17. The computer-readable medium of claim 16, wherein generating a transaction pin is accomplished by generating a pseudo-random combination of numbers and letters.

18. The computer-readable medium of claim 16, wherein generating a transaction pin is accomplished by generating a pseudo-random selection of a word or words from a dictionary.

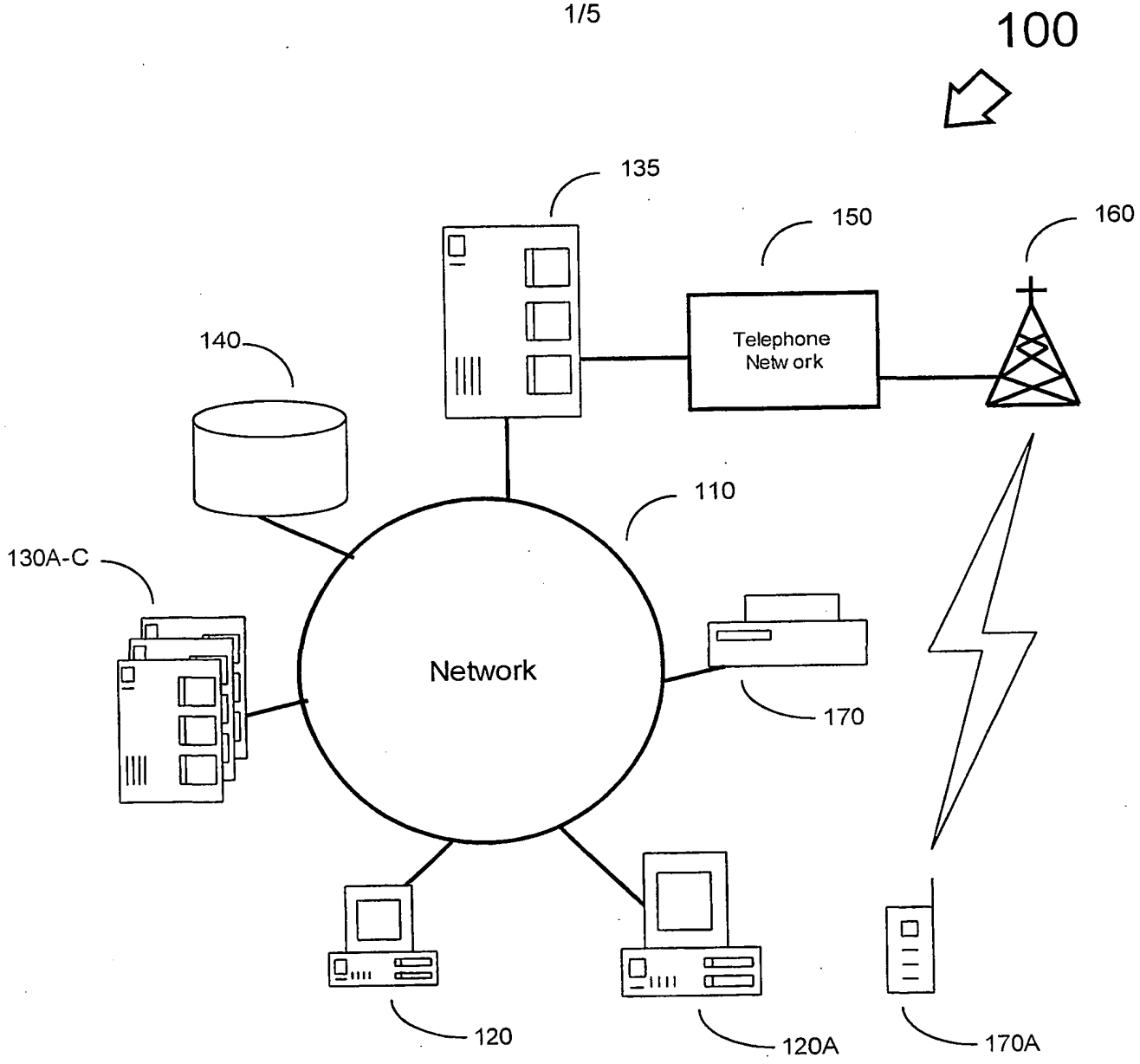

100
135
150
160
140
Telephone
Network
110
130A-C
Network
170
120
120A
170A

FIG. 1

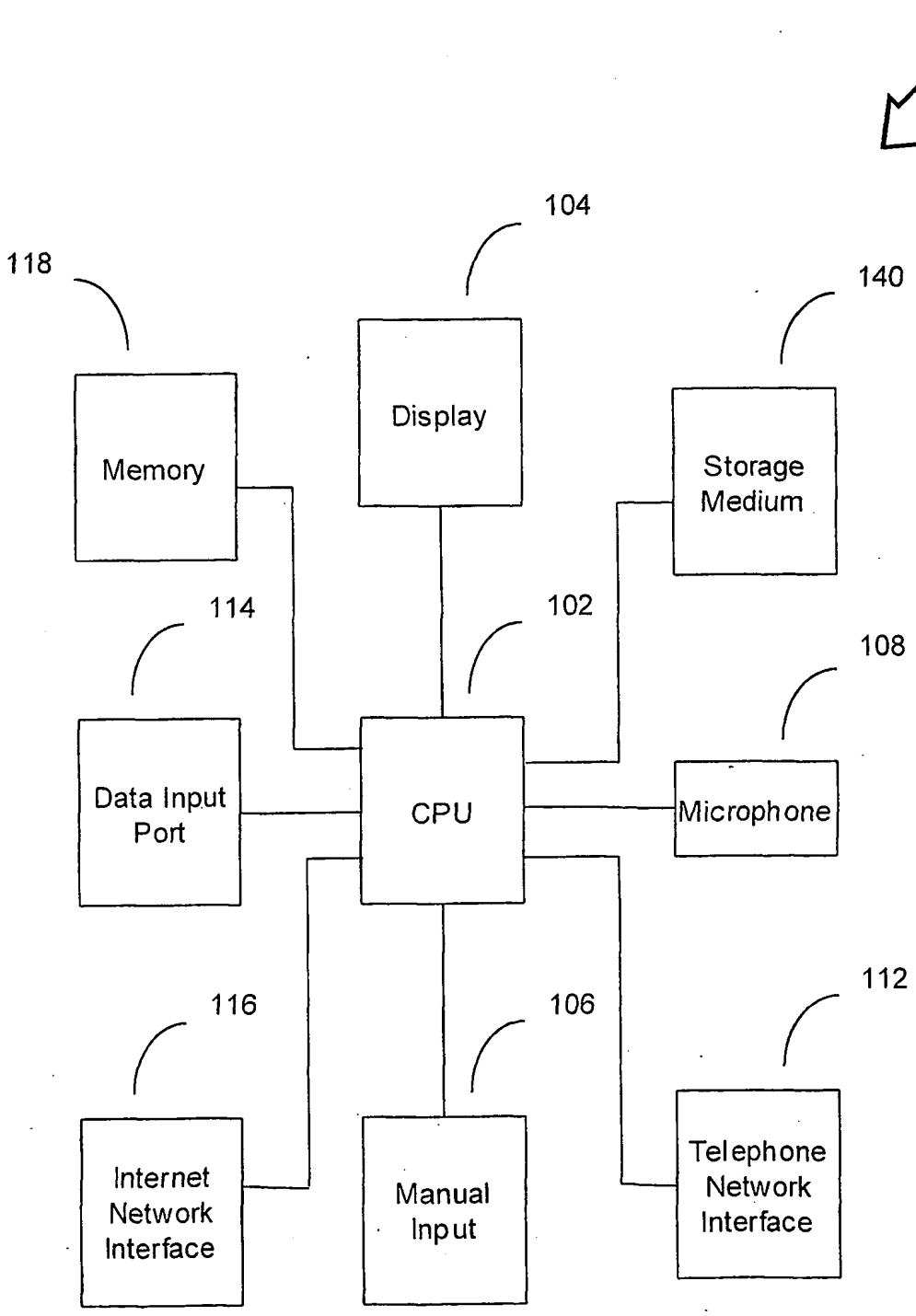

135
104
118
140
Memory
Display
Storage Medium
114
102
108
Data Input Port
CPU
Microphone
116
106
112
Internet Network Interface
Manual Input
Telephone Network Interface

FIG. 2

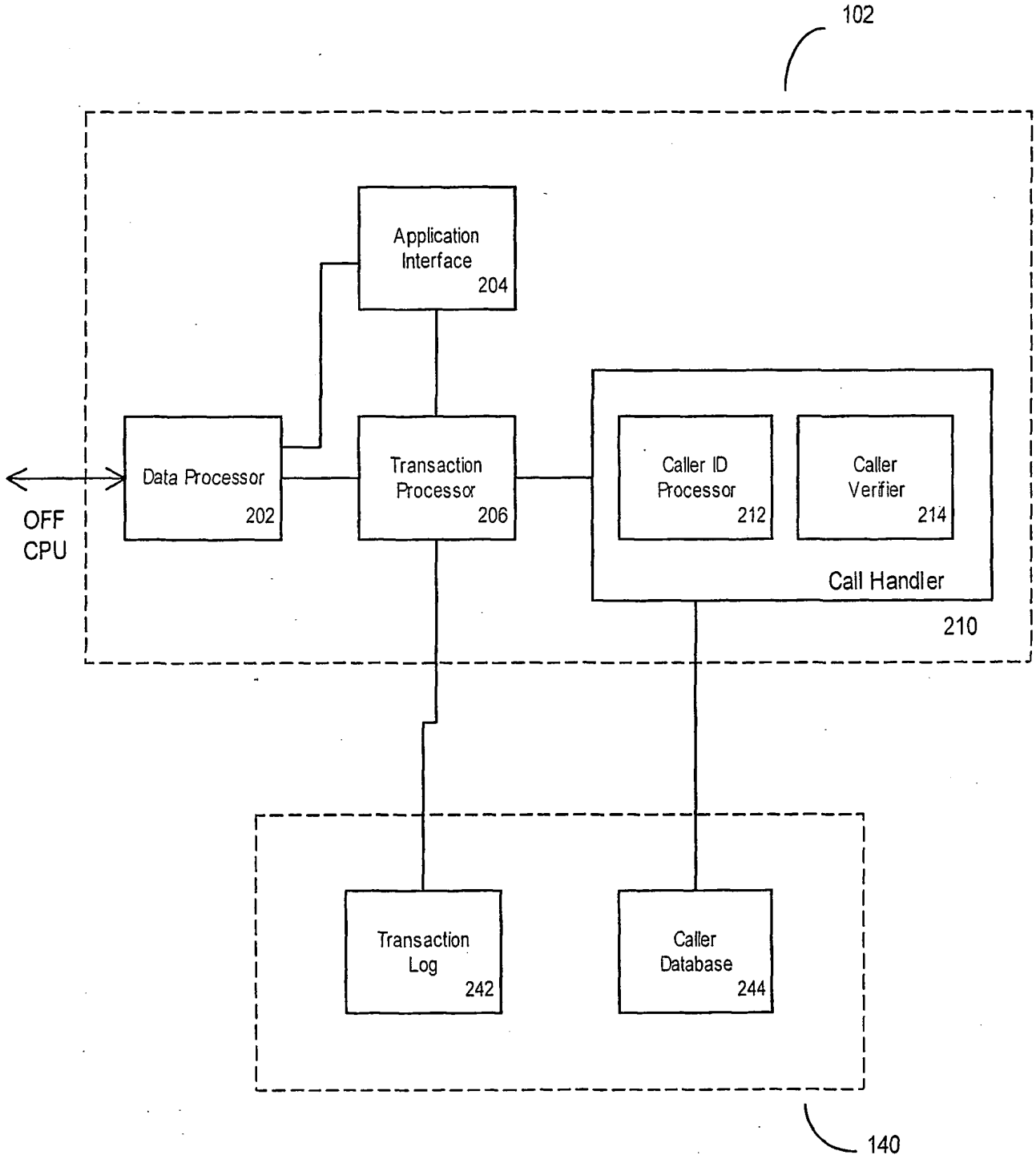

102
Application Interface 204
Data Processor 202
Transaction Processor 206
Caller ID Processor 212
Caller Verifier 214
Call Handler 210
OFF CPU
Transaction Log 242
Caller Database 244
140

FIG. 3

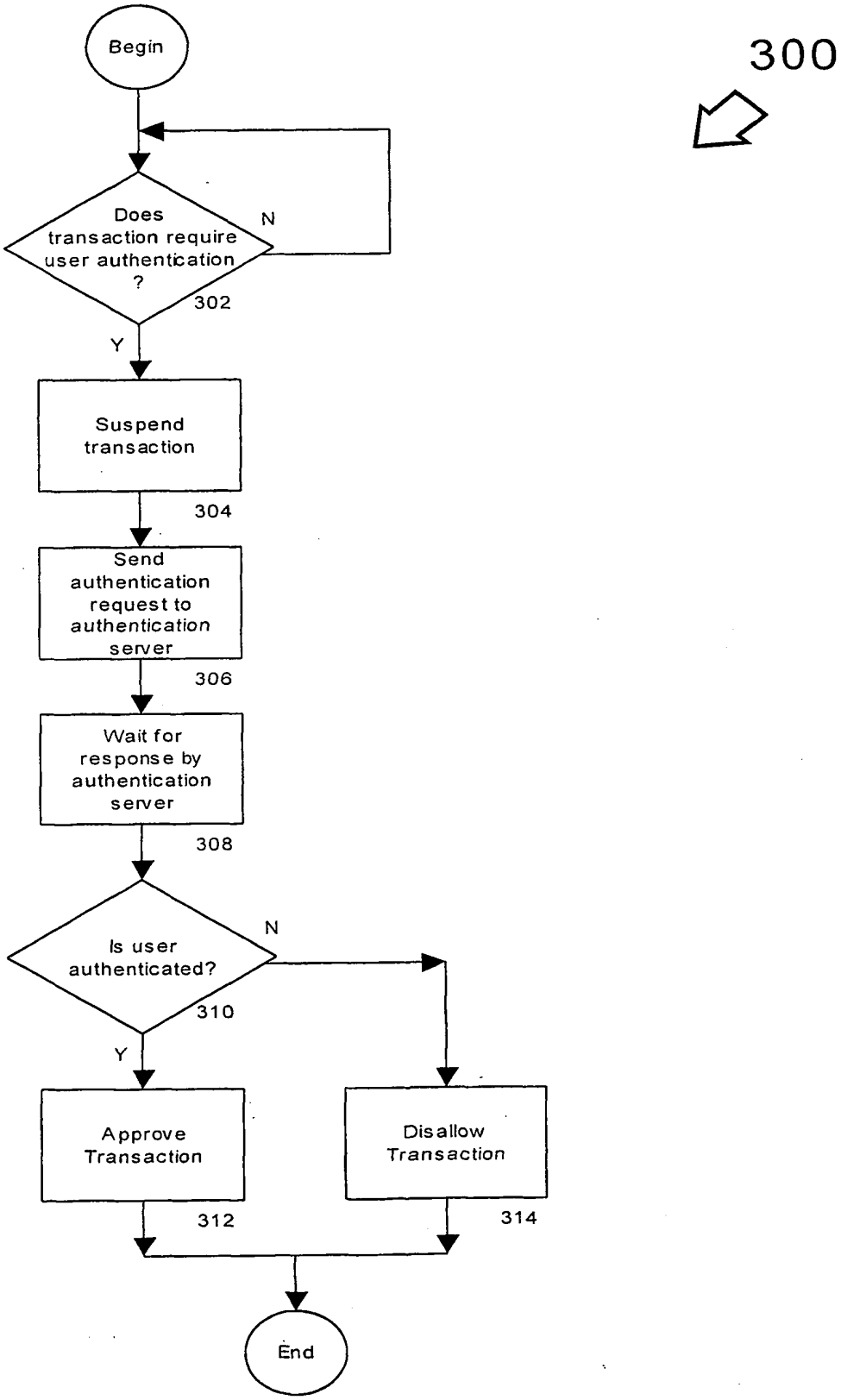

300
Begin
Does transaction require user authentication ?
N
302
Y
Suspend transaction
304
Send authentication request to authentication server
306
Wait for response by authentication server
308
Is user authenticated?
N
310
Y
Approve Transaction
312
Disallow Transaction
314
End

FIG. 4

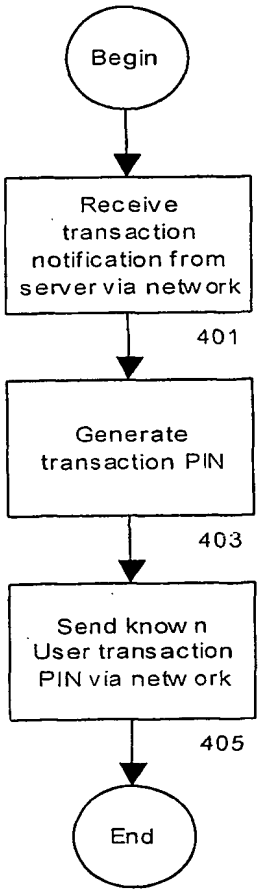

400
Begin
Receive transaction notification from server via network
401
Generate transaction PIN
403
Send known User transaction PIN via network
405
End

FIG. 5a

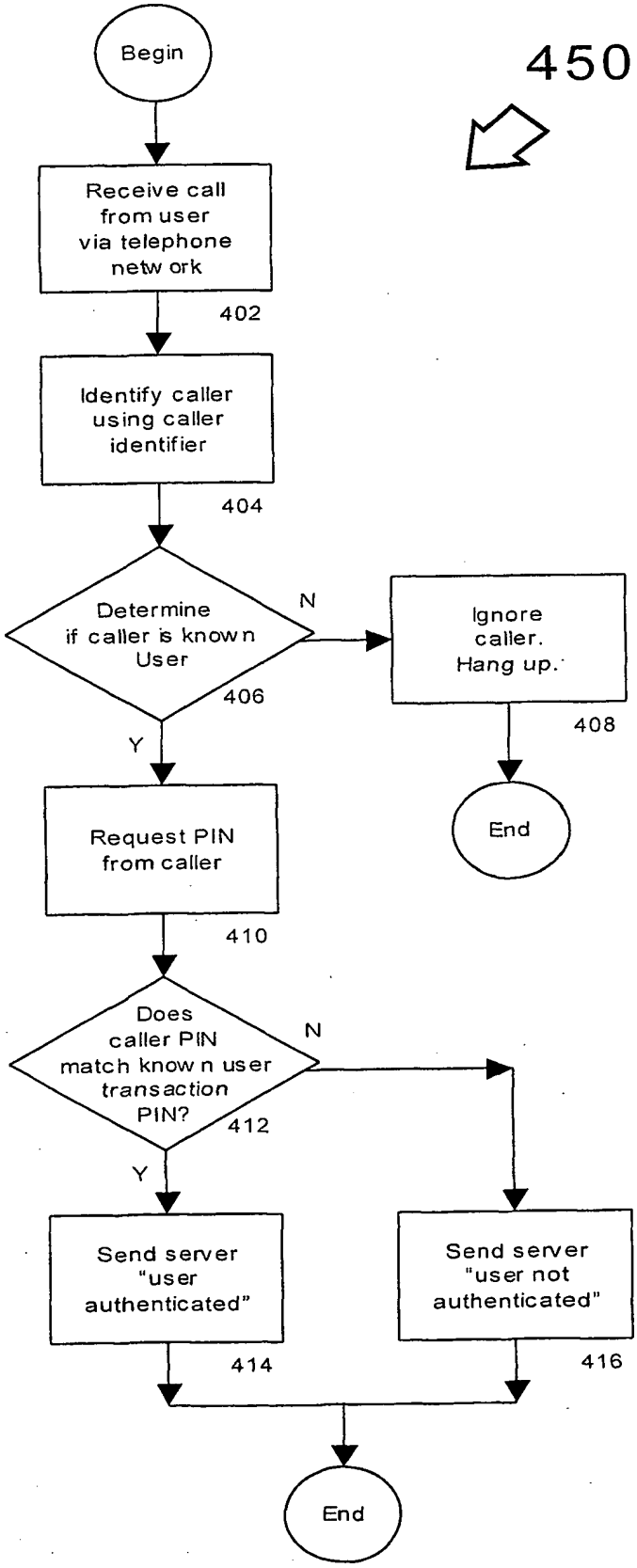

450
Begin
Receive call from user via telephone network
402
Identify caller using caller identifier
404
Determine if caller is known User
406
N
Ignore caller. Hang up.
408
End
Y
Request PIN from caller
410
Does caller PIN match known user transaction PIN?
412
N
Y
Send server "user authenticated"
414
Send server "user not authenticated"
416
End

FIG. 5b